顔認証におけるなりすまし検知に関する研究

修士学位論文要約（令和３年３月）

顔認証におけるなりすまし検知に関する研究

木村 朝輝
指導教員：青木 孝文

Spoofing Detection in Face Recognition

Asateru KIMURA
Supervisor: Takafumi AOKI

Face recognition is highly receptive and convenient. On the other hand, in face recognition, there is a risk that a malicious attacker impersonates the registrant. Many methods using the Convolutional Neural Network (CNN) have been studied as spoofing detection methods. The method using CNN has a problem that the detection accuracy is decreased against an unknown spoofing attack. In addition, it is necessary to increase the number of frames in order to extract temporal features. In this paper, we consider a robust method for unknown spoofing attacks by inputting a video of a small number of frames. The proposed method extracts facial features from an image of about 5 frames, where features based on optical flow and depth are used in combination. In order to improve the detection accuracy for unknown spoofing attacks, the proposed method employs deep metric learning in training. Through a set of experiments using the large-scale public dataset, we demonstrate the effectiveness of the proposed method.

1. はじめに

個人の身体的および行動的特徴を用いたバイオメトリクス認証は，信頼性が高く，利便性に優れているため，新しい個人認証方式として注目されている [1]. 代表的なバイオメトリクス認証の 1 つである顔認証は，低コストかつ非接触で認証可能であり，実用化が進んでいる. 顔認証は利便性と受容性に優れる認証方式であるが，悪意のある第三者が登録者になりすます危険性がある [2,3]. このような生体認証への攻撃はなりすまし攻撃と呼ばれる. 顔認証システムに対するなりすまし攻撃には，印刷された登録者の顔写真を提示する Print-Attack と登録者の顔が映った動画像を提示する Display-Attack がある. そのため，カメラで撮影された画像に写っている顔が本物であるかなりすましであるかを認証を行う前に判定する必要がある. これをなりすまし検知と呼ぶ. なりすまし検知では，Convolutional Neural Network (CNN) を用いる手法が主流である. CNN を用いた手法は，学習データに基づいて最適な特徴量を抽出できるため，従来の汎用的な画像特徴量を用いた手法よりも精度が高い. 一方で，CNN を用いた手法は，未知のなりすまし攻撃に対して検知精度が低下する問題がある. また，時間的特徴を抽出するため多数のフレームを入力する必要がある. これに対して，本論文では，少数フレームの動画像を入力とし，未知のなりすましに対してロバストな手法を検討する. 提案手法では，5 フレームの動画像から抽出される顔のテクスチャ特徴量，オプティカルフローに基づく特徴量，デプスに基づく特徴量を組み合わせて用いる. 未知のなりすまし攻撃に対する検知精度を向上させるため，ディープメトリックラーニングを用いて提案手法を学習させる. 大規模データセットを用いた性能評価実験を通して，提案手法の有効性を示す [4].

2. 深層学習を用いたなりすまし検知手法

本節では，提案手法で用いるネットワークアーキテクチャとディープメトリックラーニングについて述べる. 提案ネットワークアーキテクチャに対してディープメトリックラーニングを用いることで，未知のなりすまし攻撃に対して検知精度の高い CNN を実現する.

(i) ネットワークアーキテクチャ

図 1 にネットワークアーキテクチャの概要を示す. AlexNet(2+1)D，FlowNetS [5]，DepthNet からそれぞれ空間的特徴量・時間的特徴量，オプティカルフローに基づく特徴量，顔のデプスに基づく特徴量を抽出する. これらの特徴を結合し，最終的な出力とする.

(ii) ディープメトリックラーニング

ディープメトリックラーニングとは，特徴空間にお

表 1　従来手法との性能比較実験結果

Prot.	Method	# of frames	APCER [%]	BPCER [%]	ACER [%]
1	FAS-BAS [6]	about 100	3.58	**3.58**	3.58
	Proposed	5	**0.70**	6.11	**3.41**
2	FAS-BAS [6]	about 100	0.57±0.69	0.57±0.69	0.57±0.69
	Proposed	5	**0.44±0.11**	**0.56±0.10**	**0.50±0.11**
3	FAS-BAS [6]	about 100	**8.31±3.81**	8.31±3.80	**8.31±3.81**
	Proposed	5	18.30±6.21	**0.61±0.21**	9.45±3.01

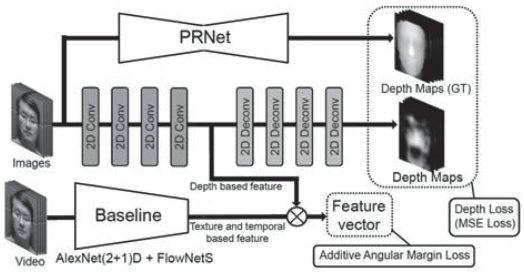

図 1　ネットワークの概要

いて，特徴間の距離や角度などを考慮した学習手法である．具体例として，クラス内分散を小さく，クラス間分散を大きくする手法が挙げられる．

提案手法では，ディープメトリックラーニングの 1 つである ArcFace [7] を用いる．ArcFace は，以下の式で表される損失に従って，クラス内分散を小さく，クラス間分散を大きくするように CNN を学習する．

$$L_{\cos} = -\frac{1}{N}\sum_{i=1}^{N}\log\frac{e^{s\{\cos(\theta_{y_i}+m)\}}}{e^{s\{\cos(\theta_{y_i}+m)\}}+\sum_{j=1,j\neq y_i}^{n}e^{s(\cos\theta_j)}}$$

ここで，θ_i は入力された特徴ベクトルとクラス i の特徴ベクトルの角度，N はバッチサイズ，s はスケーリングパラメータ，m は ArcFace におけるペナルティを表すパラメータを示す．

3.　大規模データセットを用いた性能評価実験

実験には，SiW データセット [6] を用いる．SiW データセット は，165 人分の本物，Print-Attack，Display-Attack の動画像で構成される．性能評価実験は，様々ななりすまし攻撃に対する汎化性能の評価を目的とした SiW 評価プロトコルに従う．プロトコル 1 では，未知の顔の角度や表情，姿勢などに対する汎化性能を評価する．プロトコル 2 では，Display-Attack において未知の表示ディスプレイに対する性能評価を行う．プロトコル 3 では，未知のなりすまし攻撃に対しての性能評価を行う．

従来手法である FAS-BAS [6] と提案手法の性能評価実験の結果を表 1 に示す．プロトコル 1，2 において，提案手法は，従来手法よりも高精度であった．プロトコル 3 において，5 フレームを入力とする提案手法は，100 フレーム程度の入力を必要とする従来手法と同程度に検知が可能である．表 1 から明らかなように提案手法は少数のフレームから様々ななりすまし攻撃に対して高精度に検知可能である．これは，実システムにおいて実行時間の少ない検知手法の実現に有用である．

4.　まとめ

本論文では，ディープメトリックラーニングを用いたなりすまし検知手法を提案し，大規模データセットを用いた性能評価実験を通して，提案手法の有効性を実証した．今後の展望として，他の異常検知への応用が考えられる．

文献

1) A.K. Jain, P. Flynn, and A.A. Ross, Handbook of Biometrics, Springer, 2008.
2) S. Marcel, M.S. Nixon, and S.Z. Li, Handbook of Biometric Anti-Spoofing, Springer, 2014.
3) R. Jiang, S. Al-maadeed, A. Bouridane, D. Crookes, and A. Beghdadi, Biometric Security and Privacy, Springer, 2017.
4) 木村朝輝, 伊藤康一, 青木孝文, “顔動画像の少数フレームからのなりすまし検知に関する検討,” 2020 年度暗号と情報セキュリティシンポジウム, no.1E2-3, pp.1–7, Jan. 2020.
5) A. Dosovitskiy, P. Fischer, E. Ilg, P. Häusser, C. Hazirbas, V. Golkov, P.V.D Smagt, D. Cremers, and T. Brox, “FlowNet: Learning optical flow with convolutional networks,” Proc. IEEE Int’l Conf. Computer Vision, pp.2758–2766, Dec. 2015.
6) Y. Liu, A. Jourabloo, and X. Liu, “Learning deep models for face anti-spoofing: Binary or auxiliary supervision,” Proc. IEEE/CVF Conf. Computer Vision and Pattern Recognition, pp.389–398, June 2018.
7) J. Deng, J. Guo, N. Xue, and S. Zafeiriou, “ArcFace: Additive angular margin loss for deep face recognition,” Proc. IEEE Conf. Computer Vision and Pattern Recognition, pp.4690–4699, June 2019.